National Critical Information Infrastructure Protection Centre
CVE Report
CV Scoring Scale : 3-10 01-30 Apr 2018 Vol. 05 No.08

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Application					
Apple					
Safari					
NA	2018-04-03	4.3	An issue was discovered in certain Apple products. Safari before 11.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar via a crafted web site. **CVE ID: CVE-2018-4116**	https://support.apple.com/HT208695	A-App-Safa-01052018/01
NA	2018-04-03	4.3	An issue was discovered in certain Apple products. Safari before 11.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar via a crafted web site. **CVE ID:CVE-2018-4102**	https://support.apple.com/HT208695	A-App-Safa-01052018/02
DoS Exec Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID:CVE-2017-7071**	https://support.apple.com/HT207600	A-App-Safa-01052018/03
Cacti					
Cacti					
XSS	2018-04-12	3.5	Cacti before 1.1.37 has XSS because it makes certain htmlspecialchars calls without the ENT_QUOTES flag (these calls occur when the html_escape function in lib/html.php is not used).**CVE ID:CVE-2018-10061**	NA	A-Cac-Cact-01052018/04
XSS	2018-04-12	3.5	Cacti before 1.1.37 has XSS because it does not properly reject unintended characters, related to use of the sanitize_uri function in lib/functions.php. **CVE ID:CVE-2018-10060**	NA	A-Cac-Cact-01052018/05

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
XSS	2018-04-12	3.5	Cacti before 1.1.37 has XSS because the get_current_page function in lib/functions.php relies on $_SERVER['PHP_SELF'] instead of $_SERVER['SCRIPT_NAME'] to determine a page name. **CVE ID: CVE-2018-10059**	NA	A-Cac-Cact-01052018/06
Cmsmadesimple					
Cms Made Simple					
XSS	2018-04-11	3.5	CMS Made Simple (aka CMSMS) 2.2.7 has Stored XSS in admin/siteprefs.php via the metadata parameter. **CVE ID: CVE-2018-10033**	https://github.com/zxyxx/cmsms_vul	A-Cms-CmsM-01052018/07
XSS	2018-04-11	3.5	CMS Made Simple (aka CMSMS) 2.2.7 has Reflected XSS in admin/moduleinterface.php via the m1_version parameter. **CVE ID: CVE-2018-10032**	https://github.com/zxyxx/cmsms_vul	A-Cms-CmsM-01052018/08
XSS	2018-04-11	3.5	CMS Made Simple (aka CMSMS) 2.2.7 has Reflected XSS in admin/moduleinterface.php via the m1_name parameter, related to moduledepends, a different vulnerability than CVE-2017-16799.**CVE ID:CVE-2018-10029**	https://github.com/zxyxx/cmsms_vul	A-Cms-CmsM-01052018/09
Gain Information	2018-04-13	5	CMS Made Simple (CMSMS) through 2.2.7 allows physical path leakage via an invalid /index.php?page= value, a crafted URI starting with /index.php?mact=Search, or a direct request to /admin/header.php, /admin/footer.php, /lib/tasks/class.ClearCache.task.php, or /lib/tasks/class.CmsSecurityCheck.task.php.**CVE ID:CVE-2018-10082**	https://github.com/itodaro/cve/blob/master/README.md	A-Cms-CmsM-01052018/10
NA	2018-04-13	5	CMS Made Simple (CMSMS) through 2.2.6 contains an admin password reset vulnerability because data values are improperly compared, as demonstrated by a hash beginning with the "0e" substring. **CVE ID: CVE-2018-10081**	https://github.com/itodaro/cve/blob/master/README.md	A-Cms-CmsM-01052018/11

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Dir. Trav.	2018-04-13	6.4	CMS Made Simple (CMSMS) through 2.2.7 contains an arbitrary file deletion vulnerability in the admin dashboard via directory traversal sequences in the val parameter within a cmd=del request, because code under modules\FilePicker does not restrict the val parameter. **CVE ID: CVE-2018-10083**	https://github.com/itodaro/cve/blob/master/README.md	A-Cms-CmsM-01052018/12
Execute Code Bypass	2018-04-13	6.5	CMS Made Simple (CMSMS) through 2.2.7 contains an arbitrary code execution vulnerability in the admin dashboard because the implementation uses "eval('function testfunction'.rand()" and it is possible to bypass certain restrictions on these "testfunction" functions. **CVE ID: CVE-2018-10086**	https://github.com/itodaro/cve/blob/master/README.md	A-Cms-CmsM-01052018/13
Bypass	2018-04-13	6.5	CMS Made Simple (CMSMS) through 2.2.6 contains a privilege escalation vulnerability from ordinary user to admin user by arranging for the eff_uid value within $_COOKIE[$this->_loginkey] to equal 1, because an SHA-1 cryptographic protection mechanism can be bypassed. **CVE ID: CVE-2018-10084**	https://github.com/itodaro/cve/blob/master/README.md	A-Cms-CmsM-01052018/14
CSRF	2018-04-11	6.8	CMS Made Simple (aka CMSMS) 2.2.7 has CSRF in admin/moduleinterface.php. **CVE ID: CVE-2018-10031**	https://github.com/zxyxx/cmsms_vul	A-Cms-CmsM-01052018/15
CSRF	2018-04-11	6.8	CMS Made Simple (aka CMSMS) 2.2.7 has CSRF in admin/siteprefs.php. **CVE ID: CVE-2018-10030**	https://github.com/zxyxx/cmsms_vul	A-Cms-CmsM-01052018/16
Execute Code	2018-04-13	7.5	CMS Made Simple (CMSMS) through 2.2.6 allows PHP object injection because of an unserialize call in the _get_data function of \lib\classes\internal\class.LoginOperations.php. By sending a crafted cookie, a remote attacker can upload and execute code, or delete files. **CVE ID: CVE-2018-10085**	https://github.com/itodaro/cve/blob/master/README.md	A-Cms-CmsM-01052018/17

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Dsmall Project					
Dsmall					
XSS	2018-04-04	4.3	dsmall v20180320 allows XSS via the pdr_sn parameter to public/index.php/home/predeposit/index.html. **CVE ID: CVE-2018-9307**	https://github.com/xuheunbaicai/cangku/blob/master/cve/%E9%AD%94%E6%96%B9%E5%8A%A8%E5%8A%9B_Latest%20version_bug.md	A-Dsm-Dsma-01052018/18
Exiv2					
Exiv2					
DoS	2018-04-04	4.3	In Exiv2 0.26, a divide by zero in BigTiffImage::printIFD in bigtiffimage.cpp could result in denial of service. **CVE ID: CVE-2018-9304**	NA	A-Exi-Exiv-01052018/19
NA	2018-04-04	4.3	In Exiv2 0.26, an assertion failure in BigTiffImage::readData in bigtiffimage.cpp results in an abort.**CVE ID:CVE-2018-9303**	https://github.com/xiaoqx/pocs/blob/master/exiv2/readme.md	A A-Exi-Exiv-01052018/20
Gain Information	2018-04-04	5.8	In Exiv2 0.26, an out-of-bounds read in IptcData::printStructure in iptc.c could result in a crash or information leak, related to the "== 0x1c" case. **CVE ID : CVE-2018-9305**	NA	A-Exi-Exiv-01052018/21
Icmsdev					
Icms					
XSS	2018-04-10	3.5	An issue was discovered in idreamsoft iCMS through 7.0.7. XSS exists via the nickname field in an admincp.php?app=user&do=save&frame=iPHP request. **CVE ID : CVE-2018-9925**	https://github.com/idreamsoft/iCMS/issues/18	A-Icm-Icms-01052018/22
Gain Information	2018-04-10	5	An issue was discovered in idreamsoft iCMS through 7.0.7. Physical path leakage exists via an invalid nickname field that reveals a core/library/weixin.class.php pathname. **CVE ID:CVE-2018-9922**	https://github.com/idreamsoft/iCMS/issues/16	A-Icm-Icms-01052018/23
CSRF	2018-04-10	6.8	An issue was discovered in idreamsoft iCMS through 7.0.7. CSRF exists in admincp.php, as demonstrated by adding an article via an app=article&do=save&frame=iPHP request. **CVE ID: CVE-2018-9923**	https://github.com/idreamsoft/iCMS/issues/17	A-Icm-Icms-01052018/24

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Sql	2018-04-10	7.5	An issue was discovered in idreamsoft iCMS through 7.0.7. SQL injection exists via the pid array parameter in an admincp.php?app=tag&do=save&frame=iPHP request. **CVE ID: CVE-2018-9924**	https://github.com/idreamsoft/iCMS/issues/19	A-Icm-Icms-01052018/25
Oracle					
Access Manager					
NA	2018-04-18	5.8	Vulnerability in the Oracle Access Manager component of Oracle Fusion Middleware (subcomponent: Web Server Plugin). Supported versions that are affected are 10.1.4.3.0, 11.1.2.3.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Access Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Access Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS 3.0 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N). **CVE ID: CVE-2018-2739**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Acce-01052018/26

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	5.8	Vulnerability in the Oracle Access Manager component of Oracle Fusion Middleware (subcomponent: Web Server Plugin). Supported versions that are affected are 10.1.4.3.0, 11.1.2.3.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N). **CVE ID: CVE-2018-2587**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Acce-01052018/27
NA	2018-04-18	6.8	Vulnerability in the Oracle Access Manager component of Oracle Fusion Middleware (subcomponent: Authentication Engine). Supported versions that are affected are 11.1.2.3.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. While the vulnerability is in Oracle Access Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Access Manager. Note: Please refer to Doc ID <a href="http://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=2386496.1">My Oracle Support Note 2386496.1 for instructions on how to address this issue. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Acce-01052018/28

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID: CVE-2018-2879**		
Adaptive Access Manager					
NA	2018-04-18	4.9	Vulnerability in the Oracle Adaptive Access Manager component of Oracle Fusion Middleware (subcomponent: OAAM Admin). The supported version that is affected is 11.1.2.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Adaptive Access Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Adaptive Access Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Adaptive Access Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Adaptive Access Manager accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N). **CVE ID: CVE-2018-2770**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Adap-01052018/29

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Agile Product Lifecycle Management For Process					
NA	2018-04-18	5.8	Vulnerability in the Oracle Agile Product Lifecycle Management for Process component of Oracle Supply Chain Products Suite (subcomponent: Installation). Supported versions that are affected are 6.1.1.6, 6.2.0.0 and 6.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile Product Lifecycle Management for Process, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile Product Lifecycle Management for Process accessible data as well as unauthorized read access to a subset of Oracle Agile Product Lifecycle Management for Process accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID: CVE-2018-2572**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Agil-01052018/30
Banking Corporate Lending;Banking Payments;Flexcube Enterprise Limits And Collateral Management;Flexcube Investor Servicing;Flexcube Universal Banking					
NA	2018-04-18	4	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0 and 14.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Bank-01052018/31

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2018-2747**		
NA	2018-04-18	4.9	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0 and 14.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Corporate Lending, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID: CVE-2018-2749**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Bank-01052018/32
NA	2018-04-18	5.5	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0 and 14.0.0. Easily exploitable vulnerability allows low privileged attacker with network	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Bank-

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Corporate Lending accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE ID: CVE-2018-2746**		01052018/33
NA	2018-04-18	5.8	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0 and 14.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Corporate Lending, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID: CVE-2018-2748**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Bank-01052018/34

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Communications Order And Service Management					
NA	2018-04-18	4.9	Vulnerability in the Oracle Communications Order and Service Management component of Oracle Communications Applications (subcomponent: WebUI). Supported versions that are affected are 7.2.4.3.0, 7.3.0.1.x, 7.3.1.0.7 and 7.3.5.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Order and Service Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications Order and Service Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Communications Order and Service Management accessible data. CVSS 3.0 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N). **CVE ID: CVE-2018-2756**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Comm-01052018/35

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
E-business Suite					
NA	2018-04-18	5	Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Account Hierarchy Manager). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle General Ledger accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2018-2873**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-E-bus-01052018/36
NA	2018-04-18	5	Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Account Hierarchy Manager). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle General Ledger accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID: CVE-2018-2872**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-E-bus-01052018/37

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Gain Information	2018-04-18	5	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Diagnostics). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID: CVE-2018-2867**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-E-bus-01052018/38
NA	2018-04-18	5	Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Consolidation Hierarchy Viewer). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle General Ledger accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID: CVE-2018-2866**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-E-bus-01052018/39
NA	2018-04-18	5		http://www.oracle.co	A-Ora-E-

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Consolidation Hierarchy Viewer). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle General Ledger accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID: CVE-2018-2865**	m/technetwork/security-advisory/cpuapr2018-3678067.html	bus-01052018/40
Enterprise Manager Base Platform					
DoS	2018-04-18	6.8	Vulnerability in the Enterprise Manager Base Platform component of Oracle Enterprise Manager Products Suite (subcomponent: UI Framework). The supported version that is affected is 12.1.0.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Enterprise Manager Base Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Base Platform	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Ente-01052018/41

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			accessible data as well as unauthorized read access to a subset of Enterprise Manager Base Platform accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Enterprise Manager Base Platform. CVSS 3.0 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2018-2750**		
Hospitality Cruise Fleet Management					
DoS	2018-04-18	7.5	Vulnerability in the Enterprise Manager Ops Center component of Oracle Enterprise Manager Products Suite (subcomponent: Framework). Supported versions that are affected are 12.2.2 and 12.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Ops Center. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Ops Center accessible data as well as unauthorized read access to a subset of Enterprise Manager Ops Center accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Enterprise Manager Ops Center. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2018-2742**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/42
Hospitality Guest Access					
DoS	2018-04-18	7.5	Vulnerability in the Oracle Hospitality Cruise Fleet Management System component of Oracle Hospitality Applications (subcomponent: Fleet Management System Suite). The	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/43

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			supported version that is affected is 9.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Hospitality Cruise Fleet Management System. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Fleet Management System accessible data as well as unauthorized read access to a subset of Oracle Hospitality Cruise Fleet Management System accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Cruise Fleet Management System. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2018-2850**		
Hospitality Simphony					
NA	2018-04-18	5.5	Vulnerability in the Oracle Hospitality Guest Access component of Oracle Hospitality Applications (subcomponent: Base). Supported versions that are affected are 4.2.0 and 4.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Guest Access. While the vulnerability is in Oracle Hospitality Guest Access, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Guest Access accessible data as well as unauthorized read access to a subset of Oracle Hospitality Guest Access accessible data. CVSS 3.0	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/44

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2852**		
NA	2018-04-18	4	Vulnerability in the Oracle Hospitality Simphony First Edition component of Oracle Hospitality Applications (subcomponent: Operations). Supported versions that are affected are 1.6 and 1.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony First Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony First Edition accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : VE-2018-2847**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/45
NA	2018-04-18	4	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Enterprise Management Console). Supported versions that are affected are 2.8, 2.9 and 2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony. While the vulnerability is in Oracle Hospitality Simphony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/46

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			accessible data. CVSS 3.0 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2018-2824**		
NA	2018-04-18	5	Vulnerability in the Oracle Hospitality Simphony First Edition component of Oracle Hospitality Applications (subcomponent: Client Application Loader). Supported versions that are affected are 1.6 and 1.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony First Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony First Edition accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2018-2848**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/47
NA	2018-04-18	5.5	Vulnerability in the Oracle Hospitality Simphony First Edition component of Oracle Hospitality Applications (subcomponent: Operations, Client Application Loader). Supported versions that are affected are 1.6 and 1.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony First Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Simphony First Edition accessible data as well as unauthorized read access to a	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/48

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			subset of Oracle Hospitality Simphony First Edition accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2853**		
NA	2018-04-18	5.5	Vulnerability in the Oracle Hospitality Simphony First Edition component of Oracle Hospitality Applications (subcomponent: Enterprise Management Console). Supported versions that are affected are 1.6 and 1.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony First Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Simphony First Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Simphony First Edition accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2018-2851**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/49
NA	2018-04-18	5.5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Enterprise Management Console). Supported versions that are affected are 2.7, 2.8, 2.9 and 2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/50

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			or all Oracle Hospitality Simphony accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/ S:U/C:H/I:H/A:N). **CVE ID : CVE-2018-2833**		
NA	2018-04-18	5.5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Client Application Loader). Supported versions that are affected are 2.8 and 2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Simphony accessible data as well as unauthorized read access to a subset of Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/ S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2802**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/51
DoS	2018-04-18	7.5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Enterprise Management Console). The supported version that is affected is 2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony accessible data as well as	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Hosp-01052018/52

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle Hospitality Simphony accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Simphony. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2018-2829**		
Http Server					
NA	2018-04-18	4.3	Vulnerability in the Oracle HTTP Server component of Oracle Fusion Middleware (subcomponent: OSSL Module). Supported versions that are affected are 12.1.3 and 12.2.1.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2018-2760**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Http-01052018/53
JDK;JRE					

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	5.1	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2826**	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/54

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	5.1	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2825**	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-jdk;-01052018/55
Mysql					
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Mysq-01052018/56

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE-2018-2759		
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: GIS Extension). Supported versions that are affected are 5.6.39 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2805**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Ora-Mysq-01052018/57
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2758**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Ora-Mysq-01052018/58
Outside In Technology					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS	2018-04-18	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE ID : CVE-2018-2806**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Outs-01052018/59
DoS	2018-04-18	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Image Export SDK). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker.	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Outs-01052018/60

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE ID : CVE-2018-2801**		
DoS	2018-04-18	5.8	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Outs-01052018/61

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE ID : CVE-2018-2768**		
Peoplesoft Enterprise Human Capital Management					
NA	2018-04-18	4.9	Vulnerability in the PeopleSoft Enterprise HCM component of Oracle PeopleSoft Products (subcomponent: Security). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2752**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/62
Peoplesoft Enterprise Human Capital Management Shared Components					

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	5.8	Vulnerability in the PeopleSoft Enterprise HCM Shared Components component of Oracle PeopleSoft Products (subcomponent: Notepad). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Shared Components. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Shared Components, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Shared Components accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Shared Components accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2878**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/63
Peoplesoft Enterprise Peopletools					
Gain Information	2018-04-18	4	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Core). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data.	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/64

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2018-2820**		
NA	2018-04-18	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Homepage & Navigation). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2018-2809**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/65
NA	2018-04-18	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Stylesheet). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/66

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2018-2785**		
NA	2018-04-18	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Rich Text Editor). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2821**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/67
NA	2018-04-18	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Core). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/68

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2788**		
NA	2018-04-18	6.5	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Rich Text Editor). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2018-2772**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/69
DoS	2018-04-18	7.5	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: SQR). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/70

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PT PeopleTools. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2018-2774**		
Peoplesoft Enterprise Prtl Interaction Hub					
NA	2018-04-18	5.8	Vulnerability in the PeopleSoft Enterprise PRTL Interaction Hub component of Oracle PeopleSoft Products (subcomponent: EPPCM_HIER_TOP). The supported version that is affected is 9.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PRTL Interaction Hub. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PRTL Interaction Hub, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PRTL Interaction Hub accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PRTL Interaction Hub	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Peop-01052018/71

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2838**		
Retail Central Office					
NA	2018-04-18	6.4	Vulnerability in the Oracle Retail Central Office component of Oracle Retail Applications (subcomponent: Security). Supported versions that are affected are 13.4.9, 14.0.4 and 14.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Central Office. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Central Office accessible data as well as unauthorized read access to a subset of Oracle Retail Central Office accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2738**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Reta-01052018/72
Retail Returns Management					
NA	2018-04-18	6.4	Vulnerability in the Oracle Retail Returns Management component of Oracle Retail Applications (subcomponent: Security). Supported versions that are affected are 2.3.8, 2.4.9, 14.0.4 and 14.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Returns Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Returns Management accessible data as well as	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Reta-01052018/73

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Retail Returns Management accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2737**		
Security Service					
NA	2018-04-18	5	Vulnerability in the Oracle Security Service component of Oracle Fusion Middleware (subcomponent: Oracle SSL API). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Security Service. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Security Service accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2018-2765**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Secu-01052018/74
Siebel Core-server Framework					
NA	2018-04-18	4	Vulnerability in the Siebel Core - Server Framework component of Oracle Siebel CRM (subcomponent: Services). The supported version that is affected is 17.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Core - Server Framework. While the vulnerability is in Siebel Core - Server Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel Core - Server Framework accessible data.	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Sieb-01052018/75

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			CVSS 3.0 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2018-2789**		
Solaris Cluster					
DoS	2018-04-18	4.6	Vulnerability in the Solaris Cluster component of Oracle Sun Systems Products Suite (subcomponent: Cluster Geo). The supported version that is affected is 4.3. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris Cluster executes to compromise Solaris Cluster. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Solaris Cluster accessible data as well as unauthorized update, insert or delete access to some of Solaris Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris Cluster. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2018-2822**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Sola-01052018/76
Vm Virtualbox					
NA	2018-04-18	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Vm-Vi-01052018/77

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2837**		
NA	2018-04-18	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2836**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-VmVi-01052018/78
NA	2018-04-18	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-VmVi-01052018/79

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2835**		
NA	2018-04-18	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2830**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-VmVi-01052018/80
NA	2018-04-18	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-VmVi-01052018/81

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2860**		
NA	2018-04-18	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H). **CVE ID : CVE-2018-2845**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Vm Vi-01052018/82

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2844**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-VmVi-01052018/83
NA	2018-04-18	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2843**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-VmVi-01052018/84

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.36 and Prior to 5.2.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2842**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-VmVi-01052018/85
Webcenter Sites					
NA	2018-04-18	5.8	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). Supported versions that are affected are 11.1.1.8.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 8.2	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Webc-01052018/86

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2018-2791**		
Weblogic Server					
NA	2018-04-18	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2018-2628**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Webl-01052018/87
Wireshark					
Wireshark					
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and	NA	A-Wir-Wire-

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			2.2.0 to 2.2.13, ui/failure_message.c has a memory leak. **CVE ID : CVE-2018-9274**		01052018 /88
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-pcp.c has a memory leak. **CVE ID : CVE-2018-9273**	NA	A-Wir-Wire-01052018 /89
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-h223.c has a memory leak. **CVE ID : CVE-2018-9272**	NA	A-Wir-Wire-01052018 /90
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-multipart.c has a memory leak. **CVE ID : CVE-2018-9271**	NA	A-Wir-Wire-01052018 /91
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/oids.c has a memory leak. **CVE ID : CVE-2018-9270**	NA	A-Wir-Wire-01052018 /92
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-giop.c has a memory leak. **CVE ID : CVE-2018-9269**	NA	A-Wir-Wire-01052018 /93
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-smb2.c has a memory leak. **CVE ID : CVE-2018-9268**	NA	A-Wir-Wire-01052018 /94
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-lapd.c has a memory leak. **CVE ID : CVE-2018-9267**	NA	A-Wir-Wire-01052018 /95
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-isup.c has a memory leak. **CVE ID : CVE-2018-9266**	NA	A-Wir-Wire-01052018 /96
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-tn3270.c has a memory leak. **CVE ID : CVE-2018-9265**	NA	A-Wir-Wire-01052018 /97
Overflow	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the ADB dissector could crash with a heap-based buffer overflow. This was	NA	A-Wir-Wire-01052018 /98

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			addressed in epan/dissectors/packet-adb.c by checking for a length inconsistency. **CVE ID : CVE-2018-9264**		
	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the Kerberos dissector could crash. This was addressed in epan/dissectors/packet-kerberos.c by ensuring a nonzero key length. **CVE ID : CVE-2018-9263**	NA	A-Wir-Wire-01052018/99
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the VLAN dissector could crash. This was addressed in epan/dissectors/packet-vlan.c by limiting VLAN tag nesting to restrict the recursion depth. **CVE ID : CVE-2018-9262**	NA	A-Wir-Wire-01052018/100
Overflow	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the NBAP dissector could crash with a large loop that ends with a heap-based buffer overflow. This was addressed in epan/dissectors/packet-nbap.c by prohibiting the self-linking of DCH-IDs. **CVE ID : CVE-2018-9261**	NA	A-Wir-Wire-01052018/101
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the IEEE 802.15.4 dissector could crash. This was addressed in epan/dissectors/packet-ieee802154.c by ensuring that an allocation step occurs. **CVE ID : CVE-2018-9260**	NA	A-Wir-Wire-01052018/102
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the MP4 dissector could crash. This was addressed in epan/dissectors/file-mp4.c by restricting the box recursion depth. **CVE ID : CVE-2018-9259**	NA	A-Wir-Wire-01052018/103
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5, the TCP dissector could crash. This was addressed in epan/dissectors/packet-tcp.c by preserving valid data sources. **CVE ID : CVE-2018-9258**	NA	A-Wir-Wire-01052018/104
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5, the CQL dissector could go into an	NA	A-Wir-Wire-01052018

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			infinite loop. This was addressed in epan/dissectors/packet-cql.c by checking for a nonzero number of columns. **CVE ID : CVE-2018-9257**		/105
NA	2018-04-04	5	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the LWAPP dissector could crash. This was addressed in epan/dissectors/packet-lwapp.c by limiting the encapsulation levels to restrict the recursion depth. **CVE ID : CVE-2018-9256**	NA	A-Wir-Wire-01052018/106
Zohocorp					
Manageengine Desktop Central					
Dir. Trav.	2018-04-18	6.4	An issue was discovered in Zoho ManageEngine Desktop Central 10.0.124 and 10.0.184: directory traversal in the SCRIPT_NAME field when modifying existing scripts. **CVE ID : CVE-2018-5337**	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-Zoh-Mana-01052018/107
NA	2018-04-18	6.5	An issue was discovered in Zoho ManageEngine Desktop Central 10.0.124 and 10.0.184: database access using a superuser account (specifically, an account with permission to write to the filesystem via SQL queries). **CVE ID : CVE-2018-5340**	https://www.manageengine.com/products/desktop-central/query-restriction-bypass-vulnerability.html	A-Zoh-Mana-01052018/108
NA	2018-04-18	6.5	An issue was discovered in Zoho ManageEngine Desktop Central 10.0.124 and 10.0.184: network services (Desktop Central and PostgreSQL) running with a superuser account. **CVE ID : CVE-2018-5342**	https://www.nccgroup.trust/uk/our-research/technical-advisory-multiple-vulnerabilities-in-manageengine-desktop-central/	A-Zoh-Mana-01052018/109
NA	2018-04-18	7.5	An issue was discovered in Zoho ManageEngine Desktop Central 10.0.124 and 10.0.184: a missing server-side check on the file type/extension when uploading and modifying scripts. **CVE ID :CVE-2018-5341**	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-Zoh-Mana-01052018/110
NA	2018-04-18	7.5	An issue was discovered in Zoho ManageEngine Desktop Central 10.0.124 and 10.0.184: missing authentication/authorization for a database query mechanism. **CVE ID : CVE-2018-5338**	https://www.manageengine.com/products/desktop-central/elevation-of-privilege-vulnerability.html	A-Zoh-Mana-01052018/111
NA	2018-04-18	7.5	An issue was discovered in Zoho ManageEngine Desktop Central	https://www.manageengine.com/products	A-Zoh-Mana-

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			10.0.124 and 10.0.184: insufficient enforcement of database query type restrictions. **CVE ID : CVE-2018-5339**	/desktop-central/query-restriction-bypass-vulnerability.html	01052018/112
Application;OS					
Apple/Apple					
Apple Tv;Icloud;Itunes/Iphone Os;Mac Os X;Watchos					
Bypass Gain Information	2018-04-03	4.3	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2018-4093**	https://support.apple.com/HT208465	A-App-Appl-01052018/113
Bypass Gain Information	2018-04-03	4.3	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2018-4090**	https://support.apple.com/HT208465	A-App-Appl-01052018/114
Bypass Gain Information	2018-04-03	4.3	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2018-4104**	https://support.apple.com/HT208698	A-App-Appl-01052018/115
DoS	2018-04-03	5	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "CoreText" component. It allows remote attackers to cause a denial of service (application crash) via a crafted string. **CVE ID : CVE-2018-4142**	https://support.apple.com/HT208698	A-App-Appl-01052018/116

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Exec Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "QuartzCore" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2018-4085**	https://support.apple.com/HT208464	A-App-Appl-01052018/117
Bypass	2018-04-03	7.5	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves CFPreferences in the "System Preferences" component. It allows attackers to bypass intended access restrictions by leveraging incorrect configuration-profile persistence. **CVE ID : CVE-2018-4115**	https://support.apple.com/HT208698	A-App-Appl-01052018/118
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "File System Events" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4167**	https://support.apple.com/HT208698	A-App-Appl-01052018/119
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "NSURLSession" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4166**	https://support.apple.com/HT208698	A-App-Appl-01052018/120

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "Quick Look" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4157**	https://support.apple.com/HT208698	A-App-Appl-01052018/121
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "CoreFoundation" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4155**	https://support.apple.com/HT208698	A-App-Appl-01052018/122
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13854**	https://support.apple.com/HT208144	A-App-Appl-01052018/123
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13904**	https://support.apple.com/HT208334	A-App-Appl-01052018/124

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "CoreAnimation" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-7171**	https://support.apple.com/HT208334	A-App-Appl-01052018/125
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4082**	https://support.apple.com/HT208465	A-App-Appl-01052018/126
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4150**	https://support.apple.com/HT208698	A-App-Appl-01052018/127
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4143**	https://support.apple.com/HT208698	A-App-Appl-01052018/128

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4109**	https://support.apple.com/HT208464	A-App-Appl-01052018/129
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "Core Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4095**	https://support.apple.com/HT208464	A-App-Appl-01052018/130
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "Core Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4087**	https://support.apple.com/HT208464	A-App-Appl-01052018/131
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "CFNetwork Session" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-7172**	https://support.apple.com/HT208334	A-App-Appl-01052018/132

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Execute Code Overflow	2018-04-03	9.3	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "Security" component. A buffer overflow allows attackers to execute arbitrary code in a privileged context via a crafted app.**CVE ID : CVE-2018-4144**	https://support.apple.com/HT208697	A-App-Appl-01052018/133
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4127**	https://support.apple.com/HT208694	A-App-Appl-01052018/134
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4118**	https://support.apple.com/HT208694	A-App-Appl-01052018/135

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4165**	https://support.apple.com/HT208695	A-App-Appl-01052018/136
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4130**	https://support.apple.com/HT208698	A-App-Appl-01052018/137
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4128**	https://support.apple.com/HT208698	A-App-Appl-01052018/138
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute	https://support.apple.com/HT208698	A-App-Appl-01052018/139

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4120**		
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4119**	https://support.apple.com/HT208698	A-App-Appl-01052018/140
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4101**	https://support.apple.com/HT208698	A-App-Appl-01052018/141
NA	2018-04-03	4.3	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves a JavaScriptCore function in the "WebKit" component. It allows attackers to trigger an assertion failure by leveraging improper array indexing. **CVE ID : CVE-2018-4113**	https://support.apple.com/HT208698	A-App-Appl-01052018/142

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4163**	https://support.apple.com/HT208696	A-App-Appl-01052018/143
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4162**	https://support.apple.com/HT208696	A-App-Appl-01052018/144
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4129**	https://support.apple.com/HT208696	A-App-Appl-01052018/145

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4125**	https://support.apple.com/HT208696	A-App-Appl-01052018/146
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4122**	https://support.apple.com/HT208696	A-App-Appl-01052018/147
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4121**	https://support.apple.com/HT208696	A-App-Appl-01052018/148

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4114**	https://support.apple.com/HT208696	A-App-Appl-01052018/149
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4161**	https://support.apple.com/HT208698	A-App-Appl-01052018/150
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "JavaScriptCore" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7005**	https://support.apple.com/HT207804	A-App-Appl-01052018/151
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. Safari before 11.0.3 is affected. tvOS before 11.2.5 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and	https://support.apple.com/HT208475	A-App-Appl-01052018/152

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			application crash) via a crafted web site.**CVE ID : CVE-2018-4089**		
Bypass Gain Information	2018-04-03	4.3	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. watchOS before 4.3 is affected. The issue involves the fetch API in the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site. **CVE ID : CVE-2018-4117**	https://support.apple.com/HT208697	A-App-Appl-01052018/153
Apple/Apple;Canonical					
Apple Tv;Icloud;Itunes;Safari/Iphone Os/Ubuntu Linux					
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-13885**	https://support.apple.com/HT208334	A-App-Appl-01052018/154
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. Safari before 11.0.3 is affected. iCloud before 7.3 on Windows is affected. iTunes before 12.7.3 on Windows is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4096**	https://support.apple.com/HT208475	A-App-Appl-01052018/155

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. Safari before 11.0.3 is affected. iCloud before 7.3 on Windows is affected. iTunes before 12.7.3 on Windows is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2018-4088**	https://support.apple.com/HT208475	A-App-Appl-01052018/156
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-13884**	https://support.apple.com/HT208324	A-App-Appl-01052018/157
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7165**	https://support.apple.com/HT208334	A-App-Appl-01052018/158
Oracle/Redhat					
JDK;JRE;Jrockit/Enterprise Linux Desktop;Enterprise Linux Server;Enterprise Linux Workstation					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	5.1	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2814**	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/159
NA	2018-04-18	3.7	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Install). Supported versions that are affected are Java SE: 8u162 and 10. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks require human interaction	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Ora-Jdk;-01052018/160

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: Applies to installation process on client deployment of Java. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2811**		
NA	2018-04-18	3.7	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162, 10 and JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, JRockit executes to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/161

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			(CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2794**		
NA	2018-04-18	4	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u181, 7u171 and 8u162; JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, JRockit accessible data as well as unauthorized read access to a subset of Java SE, JRockit accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2800**	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/162

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS	2018-04-18	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2018-2815**	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/163
DoS	2018-04-18	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/164

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2018-2799**		
DoS	2018-04-18	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/165

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2018-2798**		
DoS	2018-04-18	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2018-2797**	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/166

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS	2018-04-18	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2018-2795**	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/167
DoS	2018-04-18	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/168

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2018-2796**		
NA	2018-04-18	5.8	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u161 and 8u152; Java SE Embedded: 8u152; JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be	https://security.netapp.com/advisory/ntap-20180419-0001/	A-Ora-Jdk;-01052018/169

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2018-2783**		
OS					
Apple					
Iphone Os					
Bypass	2018-04-03	7.5	An issue was discovered in certain Apple products. iOS before 11.3 is affected. The issue involves the "Web App" component. It allows remote attackers to bypass intended restrictions on cookie persistence. **CVE ID : CVE-2018-4110**	https://support.apple.com/HT208693	O-App-Ipho-01052018/170
Iphone Os;Mac Os X					
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7002**	https://support.apple.com/HT207798	O-App-Ipho-01052018/171
DoS Execute Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7001**	https://support.apple.com/HT207798	O-App-Ipho-01052018/172
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is	https://support.apple.com/HT208693	O-App-Ipho-01052018

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			affected. The issue involves the "PluginKit" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4156**		/173
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. The issue involves the "Storage" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4154**	https://support.apple.com/HT208693	O-App-Ipho-01052018/174
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. The issue involves the "iCloud Drive" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4151**	https://support.apple.com/HT208693	O-App-Ipho-01052018/175
Iphone Os;Mac Os X;Watchos					
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. iOS before 11.3 is affected. macOS before 10.13.4 is affected. watchOS before 4.3 is affected. The issue involves the "CoreFoundation" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4158**	https://support.apple.com/HT208692	O-App-Ipho-01052018/176
Mac Os X					
Bypass Gain Information	2018-04-03	4.3	An issue was discovered in certain Apple products. macOS before 10.13.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2017-7173**	https://support.apple.com/HT208331	O-App-Maco-01052018/177
Bypass Gain Information	2018-04-03	4.3	An issue was discovered in certain Apple products. macOS before 10.13.3 is affected. The issue involves the "Wi-Fi" component. It	https://support.apple.com/HT208465	O-App-Maco-01052018/178

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2018-4084**		
Bypass Gain Information	2018-04-03	4.3	An issue was discovered in certain Apple products. macOS before 10.13.4 is affected. The issue involves the "NVIDIA Graphics Drivers" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2018-4138**	https://support.apple.com/HT208692	O-App-Maco-01052018/179
Gain Information	2018-04-03	4.3	An issue was discovered in certain Apple products. macOS before 10.13.4 is affected. The issue involves the "ATS" component. It allows attackers to obtain sensitive information by leveraging symlink mishandling. **CVE ID : CVE-2018-4112**	https://support.apple.com/HT208692	O-App-Maco-01052018/180
Execute Code	2018-04-03	7.6	An issue was discovered in certain Apple products. macOS before 10.13.4 is affected. The issue involves the "Notes" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4152**	https://support.apple.com/HT208692	O-App-Maco-01052018/181
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "AppleGraphicsControl" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-13853**	https://support.apple.com/HT207922	O-App-Maco-01052018/182
Execute Code	2018-04-03	9.3	An issue was discovered in certain Apple products. macOS before 10.13.1 is affected. The issue involves the "Security" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2017-7170**	https://support.apple.com/HT208221	O-App-Maco-01052018/183

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. macOS before 10.13.3 is affected. The issue involves the "IOHIDFamily" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4098**	https://support.apple.com/HT208465	O-App-Maco-01052018/184
Execute Code	2018-04-03	9.3	An issue was discovered in certain Apple products. macOS before 10.13.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID : CVE-2018-4097**	https://support.apple.com/HT208465	O-App-Maco-01052018/185
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. macOS before 10.13.3 is affected. The issue involves the "Touch Bar Support" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4083**	https://support.apple.com/HT208465	O-App-Maco-01052018/186
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. macOS before 10.13.4 is affected. The issue involves the "kext tools" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4139**	https://support.apple.com/HT208692	O-App-Maco-01052018/187
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. macOS before 10.13.4 is affected. The issue involves the "IOFireWireFamily" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4135**	https://support.apple.com/HT208692	O-App-Maco-01052018/188
DoS Execute Code Overflow Mem. Corr.	2018-04-03	9.3	An issue was discovered in certain Apple products. macOS before 10.13.4 is affected. The issue involves the "Intel Graphics	https://support.apple.com/HT208692	O-App-Maco-01052018/189

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2018-4132**		
Cisco					
Ios Xe					
Exec Code Gain privileges	2018-04-02	7.2	Multiple vulnerabilities in the CLI parser of Cisco IOS XE Software could allow an authenticated, local attacker to inject arbitrary commands into the CLI of the affected software, which could allow the attacker to gain access to the underlying Linux shell of an affected device and execute commands with root privileges on the device. The vulnerabilities exist because the affected software does not sufficiently sanitize command arguments before passing commands to the Linux shell for execution. An attacker could exploit these vulnerabilities by submitting a malicious CLI command to the affected software. A successful exploit could allow the attacker to break from the CLI of the affected software, which could allow the attacker to gain access to the underlying Linux shell on an affected device and execute arbitrary commands with root privileges on the device. Cisco Bug IDs: CSCuz03145, CSCuz56419, CSCva31971, CSCvb09542. **CVE ID : CVE-2018-0194**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-cmdinj	O-Cis-Iosx-01052018/190
Google					
Android					
NA	2018-04-05	4.6	An elevation of privilege vulnerability in the Qualcomm QCE driver. Product: Android. Versions: Android kernel. Android ID: A-36591162. References: QC-CR#2045061. **CVE ID : CVE-2017-0751**	https://source.android.com/security/bulletin/2017-08-01	O-Goo-Andr-01052018/191
NA	2018-04-05	4.6	An elevation of privilege vulnerability in the NVIDIA firmware processing code.	https://source.android.com/security/bulletin/2017-08-01	O-Goo-Andr-01052018

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			Product: Android. Versions: Android kernel. Android ID: A-34112726. References: N-CVE-2017-0744. **CVE ID : CVE-2017-0744**		/192
Gain Information	2018-04-03	5	In Qualcomm Android for MSM, Firefox OS for MSM, and QRD Android with all Android releases from CAF using the Linux kernel before security patch level 2018-04-05, insufficient validation of parameters from userspace in the camera driver can lead to information leak and out-of-bounds access. **CVE ID : CVE-2018-3598**	https://source.android.com/security/bulletin/pixel/2018-04-01	O-Goo-Andr-01052018/193
NA	2018-04-03	5	In Qualcomm Android for MSM, Firefox OS for MSM, and QRD Android with all Android releases from CAF using the Linux kernel before security patch level 2018-04-05, a Use After Free condition can occur in the function rmnet_usb_ctrl_init(). **CVE ID : CVE-2018-3584**	https://source.android.com/security/bulletin/pixel/2018-04-01	O-Goo-Andr-01052018/194
Gain Information	2018-04-05	5	An information disclosure vulnerability in the Qualcomm audio driver. Product: Android. Versions: Android Kernel. Android ID: A-35764875. References: QC-CR#2029798. **CVE ID : CVE-2017-0748**	https://source.android.com/security/bulletin/2017-08-01	O-Goo-Andr-01052018/195
Overflow	2018-04-03	6.8	In Qualcomm Android for MSM, Firefox OS for MSM, and QRD Android with all Android releases from CAF using the Linux kernel before security patch level 2018-04-05, a buffer overwrite may occur in ProcSetReqInternal() due to missing length check. **CVE ID : CVE-2018-3566**	https://source.android.com/security/bulletin/2018-04-01	O-Goo-Andr-01052018/196
Execute Code	2018-04-03	6.8	In Qualcomm Android for MSM, Firefox OS for MSM, and QRD Android with all Android releases from CAF using the Linux kernel before security patch level 2018-04-05, untrusted pointer dereference in apr_cb_func can lead to an arbitrary code execution. **CVE ID : CVE-2018-3563**	https://source.android.com/security/bulletin/2018-04-01	O-Goo-Andr-01052018/197

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-05	6.9	In blk_mq_tag_to_rq in blk-mq.c in the upstream kernel, there is a possible use after free due to a race condition when a request has been previously freed by blk_mq_complete_request. This could lead to local escalation of privilege. Product: Android. Versions: Android kernel. Android ID: A-63083046. **CVE ID : CVE-2015-9016**	https://github.com/torvalds/linux/commit/0048b4837affd153897ed1222283492070027aa9	O-Goo-Andr-01052018/198
NA	2018-04-05	7.2	An elevation of privilege vulnerability in the NVIDIA GPU driver. Product: Android. Versions: Android kernel. Android ID: A-31799863. References: N-CVE-2016-8482. **CVE ID : CVE-2016-8482**	https://source.android.com/security/bulletin/2017-01-01	O-Goo-Andr-01052018/199
NA	2018-04-05	7.2	An elevation of privilege vulnerability in Qualcomm closed source components. Product: Android. Versions: Android kernel. Android ID: A-32573899. **CVE ID : CVE-2017-0431**	https://source.android.com/security/bulletin/2017-02-01	O-Goo-Andr-01052018/200
NA	2018-04-03	7.5	In Qualcomm Android for MSM, Firefox OS for MSM, and QRD Android with all Android releases from CAF using the Linux kernel before security patch level 2018-04-05, in MMCP, a downlink message is not being properly validated. **CVE ID : CVE-2017-18147**	https://source.android.com/security/bulletin/2018-04-01	O-Goo-Andr-01052018/201
NA	2018-04-03	7.5	In Qualcomm Android for MSM, Firefox OS for MSM, and QRD Android with all Android releases from CAF using the Linux kernel before security patch level 2018-04-05, while notifying a DCI client, a Use After Free condition can occur. **CVE ID : CVE-2018-3599**	https://source.android.com/security/bulletin/pixel/2018-04-01	O-Goo-Andr-01052018/202
NA	2018-04-03	7.5	In Qualcomm Android for MSM, Firefox OS for MSM, and QRD Android with all Android releases from CAF using the Linux kernel before security patch level 2018-04-05, legacy code vulnerable after migration has been removed. **CVE ID : CVE-2018-3596**	https://source.android.com/security/bulletin/pixel/2018-04-01	O-Goo-Andr-01052018/203
Oracle					
Solaris					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	3.6	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: ZVNET Driver). The supported version that is affected is 11.3. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Solaris accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris. CVSS 3.0 Base Score 7.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2018-2754**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	O-Ora-Sola-01052018/204
NA	2018-04-18	4.7	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11.3. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris. CVSS 3.0 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2808**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	O-Ora-Sola-01052018/205

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	4.9	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: LDAP Library). Supported versions that are affected are 10 and 11.3. Difficult to exploit vulnerability allows low privileged attacker with network access via LDAP to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2563**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	O-Ora-Sola-01052018/206
NA	2018-04-18	7.8	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via NFS to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2764**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	O-Ora-Sola-01052018/207
NA	2018-04-18	7.8	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: RPC). Supported versions that are affected are 10 and 11.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via NFS to compromise Solaris. Successful	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	O-Ora-Sola-01052018/208

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2718**		
Qualcomm					
Fsm9055 Firmware;Ipq4019 Firmware;Ipq8064 Firmware;Mdm9206 Firmware;Mdm9607 Firmware;Mdm9635m Firmware;Mdm9640 Firmware;Mdm9645 Firmware;Mdm9650 Firmware;Msm8909w Firmware;Qca4531 Firmware;Qca9980 Firmware;Sd 205 Firmware;Sd 210 Firmware;Sd 212 Firmware;Sd 400 Firmware;Sd 410 Firmware;Sd 412 Firmware;Sd 415 Firmware;Sd 425 Firmware;Sd 430 Firmware;Sd 450 Firmware;Sd 615 Firmware;Sd 616 Firmware;Sd 617 Firmware;Sd 625 Firmware;Sd 650 Firmware;Sd 652 Firmware;Sd 808 Firmware;Sd 810 Firmware;Sd 820 Firmware;Sd 835 Firmware;Sdx20 Firmware					
Overflow Mem. Corr.	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Small Cell SoC, Snapdragon Mobile, and Snapdragon Wear FSM9055, IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MSM8909W, QCA4531, QCA9980, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 835, and SDX20, improper input validation infuse read request leads to memory corruption. **CVE ID : CVE-2016-10436**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/209
NA	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Small Cell SoC, Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear FSM9055, IPQ4019, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, and SDX20, three image types are loaded in the	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/210

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			same manner without distinguishing them. **CVE ID : CVE-2016-10429**		
Gain information	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Small Cell SoC, Snapdragon Mobile, and Snapdragon Wear FSM9055, IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MSM8909W, QCA4531, QCA9980, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 835, and SDX20, information exposure vulnerability when logging debug statement due to %p usage. **CVE ID : CVE-2016-10438**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/211
NA	2018-04-18	7.5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Small Cell SoC, Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear FSM9055, IPQ4019, MDM9206, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, improper access control in system call leads to unauthorized access. **CVE ID : CVE-2016-10422**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/212
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, Snapdragon Wear, and Small Cell SoC FSM9055, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/213

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, lack of input Validation in QURTK_write() can cause potential buffer overflow. **CVE ID : CVE-2015-9224**		
Overflow	2018-04-18	7.5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Small Cell SoC, Snapdragon Mobile, and Snapdragon Wear FSM9055, MDM9206, MDM9607, MDM9615, MDM9635M, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, an integer overflow leading to buffer overflow can potentially occur in a memory API function. **CVE ID : CVE-2016-10412**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/214
Gain Information	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Small Cell SoC, Snapdragon Mobile, and Snapdragon Wear FSM9055, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 835, and SDX20, while logging debug statements or ftrace events from rmnet_data, the socket buffer function uses normal format specifiers which may result in information exposure. **CVE ID : CVE-2016-10437**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/215

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Small Cell SoC, Snapdragon Mobile, and Snapdragon Wear FSM9055, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, potential stack-based buffer overflow exist in thermal service leading to root compromise. **CVE ID : CVE-2016-10450**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/216
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile, Snapdragon Wear, and Small Cell SoC FSM9055, MDM9206, MDM9607, MDM9635M, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, and SD 835, improper input validation can occur while parsing an image. **CVE ID : CVE-2016-10501**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/217
Ipq4019 Firmware;Mdm9206 Firmware;Mdm9607 Firmware;Mdm9625 Firmware;Mdm9635m Firmware;Mdm9640 Firmware;Mdm9645 Firmware;Mdm9650 Firmware;Mdm9655 Firmware;Msm8909w Firmware;Sd 205 Firmware;Sd 210 Firmware;Sd 212 Firmware;Sd 400 Firmware;Sd 410 Firmware;Sd 412 Firmware;Sd 415 Firmware;Sd 425 Firmware;Sd 430 Firmware;Sd 450 Firmware;Sd 615 Firmware;Sd 616 Firmware;Sd 617 Firmware;Sd 625 Firmware;Sd 650 Firmware;Sd 652 Firmware;Sd 800 Firmware;Sd 808 Firmware;Sd 810 Firmware;Sd 820 Firmware;Sd 820a Firmware;Sdx20 Firmware					
NA	2018-04-18	9.3	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/218

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			SD 800, SD 808, SD 810, SD 820, SD 820A, and SDX20, in QTEE, a TOCTOU vulnerability exists due to improper access control. **CVE ID : CVE-2016-10417**		
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, and SDX20, if a RPMB listener is registered with a very small buffer size, the calculation of the maximum transfer size for read and write operations may underflow, resulting in buffer overflow. **CVE ID : CVE-2016-10484**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/219
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, if the buffer length passed to the RIL interface is too large, the buffer size calculation may overflow, resulting in an undersize allocation for the buffer, and subsequently buffer overwrite. **CVE ID : CVE-2016-10474**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm9-01052018/220
Mdm9206 Firmware;Mdm9607 Firmware;Mdm9615 Firmware;Mdm9625 Firmware;Mdm9635m Firmware;Mdm9640 Firmware;Mdm9645 Firmware;Mdm9650 Firmware;Mdm9655 Firmware;Msm8909w Firmware;Sd 205 Firmware;Sd 210 Firmware;Sd 212 Firmware;Sd 400 Firmware;Sd 410 Firmware;Sd 412 Firmware;Sd 415 Firmware;Sd 425 Firmware;Sd 430 Firmware;Sd 450 Firmware;Sd 615 Firmware;Sd 616 Firmware;Sd 617 Firmware;Sd 625 Firmware;Sd 650 Firmware;Sd 652 Firmware;Sd 800 Firmware;Sd 808 Firmware;Sd 810 Firmware;Sd 820Firmware;Sd 835 Firmware;Sd 845 Firmware;Sd 850 Firmware;Sdx20 Firmware					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Overflow Mem. Corr.	2018-04-18	7.5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, a simultaneous command post for addSA or updateSA on same SA leads to memory corruption. APIs addSA and updateSA APIs access the global variable ipsec_sa_list[] outside of mutex protection. **CVE ID : CVE-2016-10448**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/221
NA	2018-04-18	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, memory leak may occur in the IPSecurity module when repeating IKE-Rekey. **CVE ID : CVE-2016-10499**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/222
Overflow	2018-04-18	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, improper CFG allocation	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/223

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			can cause heap leak. **CVE ID : CVE-2016-10497**		
DoS	2018-04-18	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, improper initialization of ike_sa_handle_ptr in IPSEC leads to system denial of service. **CVE ID : CVE-2016-10455**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/224
DoS Overflow	2018-04-18	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, improper boundary check in RLC AM module leads to denial of service by reaching assertion. **CVE ID : CVE-2016-10427**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/225
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, key material is not always	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/226

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			cleared properly. **CVE ID : CVE-2016-10421**		
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9635M, MDM9645, MDM9650, MDM9655, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 810, SDM630, SDM636, SDM660, and Snapdragon_High_Med_2016, stopping of the DTR prematurely causes micro kernel to be stuck. This can be triggered with a timing change injectable in RACH procedure. **CVE ID : CVE-2016-10498**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/227
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, if a negative value is passed as argument "max" to qurt_qdi_state_local_new_handle_from_obj, an buffer overflow occurs, due to typecasting the signed integer to unsigned. **CVE ID : CVE-2016-10490**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/228
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Small Cell SoC, Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear FSM9055, IPQ4019, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/229

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, when a hash is passed with zero datalength, the code returns an error, even though zero data length is valid. **CVE ID : CVE-2016-10414**		
Overflow Mem. Corr.	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, NPA routines on the rootPD that handle resource requests remoted over QDI may not validate pointers passed from user space which may result in guest OS memory corruption. **CVE ID : CVE-2016-10493**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/230
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, in a QuRT API function, an untrusted pointer dereference can occur. **CVE ID : CVE-2016-10487**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/231
NA	2018-04-18	4	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9635M,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/232

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, packet replay may be possible. **CVE ID : CVE-2016-10443**		
NA	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, incorrect implementation of RSA padding functions in CORE. **CVE ID : CVE-2016-10469**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/233
NA	2018-04-18	9.3	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 820, and SD 820A, in some QTEE syscall handlers, a TOCTOU vulnerability exists. **CVE ID : CVE-2016-10435**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/234
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 820, SD 820A, SD 835, SD 845, and SD 850, upgrading LibPNG from 1.6.12 to	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/235

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			1.6.21 fixes multiple issues with different CWEs. **CVE ID : CVE-2016-10424**		
NA	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, SD 820A, and SD 835, HLOS can enable PMIC debug through TCSR_QPDI_DISABLE_CFG due to improper access control. **CVE ID : CVE-2016-10418**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/236
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, SD 820A, SD 835, SD 845, and SD 850, TZ applications are not properly validated. **CVE ID : CVE-2016-10431**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/237
NA	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 820, SD 820A, and SD 835, incorrect configuration of the OCIMEM MPU may provide NonSecure Software access to OCIMEM memory used by TZ. **CVE ID : CVE-2016-10446**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/238
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/239

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			and SD 835, if GPT listener response is passed a large buffer offset, a buffer overflow occurs. **CVE ID : CVE-2016-10425**		
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 820, SD 820A, and SD 835, SMMU Access Control Policy was updated to block HLOS from accessing BLSP and BAM resources. **CVE ID : CVE-2016-10444**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/240
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9607, MDM9615, MDM9635M, MDM9640, SD 210/SD 212/SD 205, SD 400, SD 600, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 810, and SD 820, an arbitrary length value from an incoming message to QMI Proxy can lead to an out-of-bounds write in the stack variable message. **CVE ID : CVE-2016-10479**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/241
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9615, MDM9625, MDM9635M, SD 400, SD 600, and SD 800, a buffer overflow can occur when processing an audio buffer. **CVE ID : CVE-2015-9223**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/242
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9615, MDM9625, MDM9635M, and SD 810, improper input validation can cause a null pointer dereference in USB bootloader find_ep() function. **CVE ID : CVE-2015-9215**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/243

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9635M, made changes to map the scan type value to an index value that is in range. **CVE ID : CVE-2016-10495**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/244
Overflow Mem. Corr.	2018-04-18	9.3	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9635M, MDM9640, MDM9645, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 820, and SD 820A, TOCTOU vulnerability during SSD image decryption may cause memory corruption. **CVE ID : CVE-2016-10433**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/245
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9625, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 425, SD 430, SD 450, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, integer overflow may lead to buffer overflows in IPC router Root-PD driver. **CVE ID : CVE-2016-10494**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/246
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9635M, SD 210/SD 212/SD 205, SD 410/12, SD 450, SD 615/16/SD 415, SD 625, SD 650/52, SD 808, and SD 810, A NULL pointer dereference can occur during an SSL handshake. **CVE ID : CVE-2016-10496**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/247

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9640, MDM9645, MDM9650, MDM9655, SD 450, SD 625, SD 650/52, SD 820, SD 835, SD 845, SD 850, and SDX20, when initializing scheduler object service request, an out of bounds access could occur due to uninitialized object number. **CVE ID : CVE-2016-10419**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/248
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9640, MDM9645, SD 210/SD 212/SD 205, SD 450, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, and SD 820A, PD failure reason string from user PD is used directly in root PD, so if the buffer parameter is non-NULL terminated in Diag F3 APIs, a buffer overread occurs. **CVE ID : CVE-2016-10486**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/249
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9640, SDM630, MSM8976, MSM8937, SDM845, MSM8976, and MSM8952, when running module or kernel code with improper access control allowing writing to arbitrary regions of memory, the user may utilize this vector to alter module executable code.**CVE ID : CVE-2016-10442**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/250
Gain Information	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9650, SD 210/SD 212/SD 205, SD 410/12, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, and SD 835, while printing debug message of a pointer in wlan_qmi_err_cb, the real kernel address will be printed regardless of the kptr_restrict system settings. **CVE ID : CVE-2016-10406**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/251

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9650, SD 650/52, SD 808, SD 810, SD 820, and SDX20, lack of proper bounds checking may lead to a buffer overread. **CVE ID : CVE-2016-10461**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/252
NA	2018-04-18	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, and SD 835, RTP daemon crashes and terminates VT call when UE receives RTCP unknown APP packet report which caused the parser to miss an end of RTCP packet length and go on forever looking for it, even going beyond the limits of the RTCP Packet length. **CVE ID : CVE-2016-10411**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/253
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, and SD 835, an integer overflow leading to buffer overflow can occur during a VT call.**CVE ID : CVE-2016-10407**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/254
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, SD 820, and SD 820A, function ce_pkcs1_pss_padding_verify_auto_recover_saltlen assumes that the size of the encoded message is equal to the size of the RSA modulus. This assumption is true for most RSA keys, but it fails when modulus_bitlen % 8 == 1.	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/255

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			CVE ID CVE-2016-10467		
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 210/SD 212/SD 205, SD 400, SD 430, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, and SD 820, while processing smart card requests, a buffer overflow can occur. **CVE ID : CVE-2016-10477**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/256
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 210/SD 212/SD 205, SD 400, SD 430, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, and SD 820, lack input validation may lead to a integer overflow that could potentially lead to a buffer overflow. **CVE ID : CVE-2016-10475**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/257
Overflow Mem. Corr.	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 835, SD 845, SDM630, SDM636, SDM660, SDX20, and Snapdragon_High_Med_2016, the 'proper' solution for this will be to ensure that any users of qsee_log in the bootchain (before Linux boots) unallocate their buffers and clear the qsee_log pointer. Until support for that is implemented in TZ and the bootloader, enable tz_log to avoid potential scribbling. This solution will prevent the linux kernel memory corruption. **CVE ID : CVE-2016-10458**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/258

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400, lack of address argument validation in qsee_get_tz_app_name() may lead to an untrusted pointer dereference. **CVE ID : CVE-2016-10489**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/259
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400 and SD 800, an integer overflow to buffer overflow can occur in a DRM API. **CVE ID : CVE-2015-9219**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/260
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400, SD 800, and SD 810, lack of validation of pointers passed by secure apps could lead to an untrusted pointer dereference. **CVE ID : CVE-2015-9221**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/261
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SDM630, SDM636, SDM660, and Snapdragon_High_Med_2016, the Access Control policy for HLOS allows access to Slimbus, GPU, GIC resources. **CVE ID : CVE-2016-10462**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/262
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 820, SD 820A, SD 835, SD 845, SD 850, SDM630, SDM636, SDM660, and Snapdragon_High_Med_2016, input is not properly validated in a	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/263

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			QTEE API function. **CVE ID : CVE-2016-10445**		
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, and SD 835, memory protection assertion happens after invoking TA termination out of order. **CVE ID : CVE-2016-10452**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/264
NA	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 410/12, SD 615/16/SD 415, SD 808, and SD 810, improper input validation while processing SCM Command can lead to unauthorized memory access. **CVE ID : CVE-2016-10483**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/265
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 410/12, SD 425, SD 430, SD 450, SD 617, SD 625, SD 650/52, SD 810, SD 820, and SD 820A, a buffer overflow can occur in SafeSwitch. **CVE ID : CVE-2016-10426**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/266
NA	2018-04-18	9.3	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 410/12, SD 425, SD 430, SD 450, SD 617, SD 625, SD 650/52, SD 820, and SD 820A, TOCTOU vulnerabilities may occur while sanitizing userspace values passed to tQSEE system call. **CVE ID : CVE-2016-10432**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/267
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 425, SD 430, SD 450, and SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/268

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			625, in a QTEE API function, an array out-of-bounds index can occur. **CVE ID : CVE-2016-10454**		
NA	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, and SD 650/52, there is improper access control to a bus. **CVE ID : CVE-2016-10440**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/269
Gain Inforamation	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, HMAC verification in counter file uses an insecure memcmp which may assist a timing attack. **CVE ID : CVE-2016-10428**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/270
Gain Inforamation	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, when a Trusted Application has opened the SPI interface to a particular device, it is possible for another Trusted Application to read the data on this open interface due to non-exclusive access of the SPI bus. **CVE ID : CVE-2016-10423**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/271
Gain Inforamation	2018-04-18	7.5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, when executing a TA which has been granted privileges to the CPVC MINK class it is possible for the TA to access methods exposed by the CPVC interface. **CVE ID : CVE-2016-10430**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/272

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	9.3	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, there is a TOCTOU vulnerability in the input validation for bulletin_board_read syscall. A pointer dereference is being validated without promising the pointer hasn't been changed by the HLOS program. **CVE ID : CVE-2016-10439**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/273
NA	2018-04-18	9.3	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, SD 820A, and SD 835, TOCTOU vulnerability may occur while composing the RPMB request using HLOS controlled buffers. **CVE ID : CVE-2016-10409**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm9-01052018/274
Sd 617 Firmware					
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 617, incorrect size calculation in QCRIL SCWS processing have Integer overflow which will lead to a buffer overflow. **CVE ID : CVE-2016-10478**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd61-01052018/275
Sd 820 Firmware;Sd 820a Firmware					
NA	2018-04-18	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 820 and SD 820A, the input to RPMB write response function is a buffer from HLOS that needs to be authenticated (using HMAC) and then processed. However, some of the processing occurs before the buffer is authenticated. The function will return various types of errors depending on the values of the `response` and `result` fields of the buffer before verifying the HMAC tag.	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd82-01052018/276

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			CVE ID : CVE-2016-10434		
Sd 835 Firmware;Sd 845 Firmware;Sd 850 Firmware					
Overflow	2018-04-18	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 835, SD 845, and SD 850, vendor specific opcodes may not have any packet length validation leading to buffer over-reads. **CVE ID : CVE-2016-10460**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd83-01052018/277
Application, Operating System (OS)					
Apple;Debian;Redhat/Chromium					
Iphone Os;Mac Os X/Debian Linux/Enterprise Linux Desktop;Enterprise Linux Server;Enterprise Linux Workstation/Chromium					
DoS Exec Code Overflow Mem. Corr.	2018-04-03	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7000**	https://support.apple.com/HT207797	A-App-Ipho-01052018/278
Canonical/Oracle					
Ubuntu Linux/Mysql					
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/279

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			CVE ID : CVE-2018-2780		
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2779**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/280
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2778**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/281

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2777**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/282
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via XCom to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2776**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/283
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/284

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2775**		
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2769**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/285
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2846**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/286

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2839**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/287
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2816**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/288
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/289

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2810**		
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2784**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/290
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2782**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/291

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2018-2786**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/292
NA	2018-04-18	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2018-2812**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/293
NA	2018-04-18	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/294

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2018-2787**		
NA	2018-04-18	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2766**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/295
Ubuntu Linux/Debian Linux/Mysql					
NA	2018-04-18	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Locking). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/296

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2771**		
NA	2018-04-18	3.7	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2755**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/297
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/298

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2819**		
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2818**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/299
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2817**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/300

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
NA	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2781**	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	A-Con-Ubun-01052018/301
Gain Information	2018-04-18	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2018-2813**	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/302
NA	2018-04-18	4.3	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL	https://security.netapp.com/advisory/ntap-20180419-0002/	A-Con-Ubun-01052018/303

Vulnerability Type(s)	Publish Date	CVSS	Description&CVE ID	Reference/Patch	NCIIPC ID
			Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2761**		
NA	2018-04-18	5.5	Vulnerability in the Hardware Management Pack component of Oracle Sun Systems Products Suite (subcomponent: Ipmitool). The supported version that is affected is Prior to 2.4.3. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise Hardware Management Pack. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hardware Management Pack accessible data as well as unauthorized read access to a subset of Hardware Management Pack accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2792**		A-Con-Ubun-01052018/304
Gain Information	2018-04-04	5.8	In Exiv2 0.26, an out-of-bounds read in IptcData::printStructure in iptc.c could result in a crash or information leak, related to the "!= 0x1c" case. **CVE ID : CVE-2018-9306**		A-Con-Ubun-01052018/305